What is Claimed:

1. A method for a multiparty transaction, the method comprising:

receiving at a second computing device a message from a first computing device, the message comprising multiple encrypted portions;

decrypting a first portion of the message, the first portion having first data related to a first task of the multiparty transaction and wherein the first data is decrypted using a first decryption key known to the second computing device; and

forwarding a second portion of the message to a third computing device, the second portion having second data related to a second task of the multiparty transaction and wherein the second data is decrypted using a second decryption key known to the third computing device.

2. The method of claim 1, further comprising:

receiving at the second computing device a message from the third computing device indicating a status of the second task of the multiparty transaction; and

transmitting a message from the second computing device to the first computing device indicating a status of the multiparty transaction; wherein a status the first task of the transaction and a status of the second task of the transaction are known to the second computing device.

3. The method of claim 1, further comprising:

receiving from the first computing device a message to execute the multiparty transaction; and

sending a message from the second computing device to the third computing device a message to execute the second task of the multiparty transaction.

4. The method of claim 3 wherein the message to execute the multiparty transaction is encrypted with a first encryption key and the message to execute the second task of the transaction is encrypted with a second encryption key.

5. The method of claim 1, wherein the forwarding step further comprises forwarding both the first portion of the message and the second portion of the message to the third computing device.

6. The method of claim 5, wherein the third computing device is prevented from decrypting the first portion of the message by not having access to the first decryption key.

7. The method of claim 1, wherein the second computing device is prevented from decrypting the second portion of the message by not having access to the second decryption key.

8. A method of protecting a message having information in a multiparty transaction, the method comprising:

obtaining identities of at least two transaction participants in the multiparty transaction;

obtaining cryptographic information corresponding to the at least two transaction participants;

dividing the information into segments wherein a relevant portion of the information is placed into at least two segments corresponding to the at least two identities of the transaction participants; and

cryptographically encoding the divided segments using the cryptographic information corresponding to the transaction participants.

9. The method of claim 8, wherein obtaining identities of at least two transaction participants comprises acquiring the identities from one of the transaction participants.

10. The method of claim 8, wherein obtaining cryptographic information comprises acquiring cryptographic information from at least one of a directory and cryptographic identity provider.

11. The method of claim 10, wherein the cryptographic identity provider is not one of the transaction participants.

12. The method of claim 8, wherein dividing the information into segments comprises placing only a portion of the information which is needed by a particular transaction participant into a segment encrypted for the particular participant.

13. The method of claim 8, further comprising:

transmitting a cryptographically encoded segment to only a cryptographically corresponding transaction participant.

14. The method of claim 8, further comprising:

transmitting the cryptographically encoded segments to the at least two transaction participants.

15. A method of controlling data content exposure in a multiparty transaction, the method comprising:

obtaining, from a primary transaction participant, at least two identities of secondary transaction participants to be involved in a multiparty transaction;

obtaining cryptographic information for the at least two secondary transaction participants, each secondary transaction participant having unique cryptographic information;

cryptographically encoding information for the at least two secondary transaction participants such that a data content and unique encryption are used for each secondary transaction participant; and

transmitting the cryptographically encoded information.

16. The method of claim 15, wherein transmitting the cryptographically encoded information comprises transmitting the cryptographically encoded information to the primary transaction participant.

17. The method of claim 16, further comprising:

receiving status from the primary transaction participant concerning a successful examination of data content by one or more of the at least two secondary transaction participants, whereby multiparty transaction status is assessed.

18. The method of claim 15, wherein cryptographically encoding information for the at least two secondary transaction participants comprises encoding a data content that is unique for at least one of the at least two secondary transaction participants.

19. The method of claim 15, further comprising transmitting a message request to act upon the information represented by the data content so as to execute the multiparty transaction.

20. A computer-readable medium having computer-executable instructions for performing a method for a multiparty transaction, the method comprising:

receiving at a second computing device a message from a first computing device, the message comprising multiple encrypted portions;

decrypting a first portion of the message, the first portion having first data related to a first task of the multiparty transaction and wherein the first data is decrypted using a first decryption key known to the second computing device; and

forwarding a second portion of the message to a third computing device, the second portion having second data related to a second task of the multiparty transaction and wherein the second data is decrypted using a second decryption key known to the third computing device.

21. The computer-readable medium of claim 20, further comprising method steps of:

receiving at the second computing device a message from the third computing device indicating a status of the second task of the multiparty transaction; and

transmitting a message from the second computing device to the first computing device indicating a status of the multiparty transaction; wherein a status the first task of the transaction and a status of the second task of the transaction are known to the second computing device.

22. The computer-readable medium of claim 20, further comprising method steps of:

receiving from the first computing device a message to execute the multiparty transaction; and

sending a message from the second computing device to the third computing device a message to execute the second task of the multiparty transaction.

23. The computer-readable medium of claim 20 wherein the message to execute the multiparty transaction is encrypted with a first encryption key and the message to execute the second task of the transaction is encrypted with a second encryption key.

24. The computer-readable medium of claim 20, wherein the forwarding step further comprises forwarding both the first portion of the message and the second portion of the message to the third computing device.

25. The computer-readable medium of claim 20, wherein the third computing device is prevented from decrypting the first portion of the message by not having access to the first decryption key.

26. A computer-readable medium having computer-executable instructions for performing a method of protecting a message having information in a multiparty transaction, the method comprising:

obtaining identities of at least two transaction participants in the multiparty transaction;

obtaining cryptographic information corresponding to the at least two transaction participants;

dividing the information into segments wherein a relevant portion of the information is placed into at least two segments corresponding to the at least two identities of the transaction participants; and

cryptographically encoding the divided segments using the cryptographic information corresponding to the transaction participants.

27. The computer-readable medium of claim 26, wherein obtaining identities of at least two transaction participants comprises acquiring the identities from one of the transaction participants.

28. The computer-readable medium of claim 26, wherein obtaining cryptographic information comprises acquiring cryptographic information from at least one of a directory and cryptographic identity provider.

29. The computer-readable medium of claim 26, wherein dividing the information into segments comprises placing only a portion of the information which is needed by a particular transaction participant into a segment encrypted for the particular participant.

30. The computer-readable medium of claim 26, further comprising:

transmitting a cryptographically encoded segment to only a cryptographically corresponding transaction participant.

31. The computer-readable medium of claim 26, further comprising:

transmitting the cryptographically encoded segments to the at least two transaction participants.

32. A system for a multiparty transaction, the system comprising:

a processor having access to memory, the memory having instructions which, when executed, perform the method comprising:

receiving at a second computing device a message from a first computing device, the message comprising multiple encrypted portions;

decrypting a first portion of the message, the first portion having first data related to a first task of the multiparty transaction and wherein the first data is decrypted using a first decryption key known to the second computing device; and

forwarding a second portion of the message to a third computing device, the second portion having second data related to a second task of the multiparty transaction and wherein the second data is decrypted using a second decryption key known to the third computing device.

33. The system of claim 32, wherein the instructions performing the method further comprise:

receiving at the second computing device a message from the third computing device indicating a status of the second task of the multiparty transaction; and

transmitting a message from the second computing device to the first computing device indicating a status of the multiparty transaction; wherein a status the first task of the transaction and a status of the second task of the transaction are known to the second computing device.

34. The system of claim 32, wherein the instructions performing the method further comprise:

receiving from the first computing device a message to execute the multiparty transaction; and

sending a message from the second computing device to the third computing device a message to execute the second task of the multiparty transaction.

35. A system comprising:

a processor having access to memory, the memory having instructions which, when executed, perform the method of protecting a message having information in a multiparty transaction, the method comprising:

obtaining identities of at least two transaction participants in the multiparty transaction;

obtaining cryptographic information corresponding to the at least two transaction participants;

dividing the information into segments wherein a relevant portion of the information is placed into at least two segments corresponding to the at least two identities of the transaction participants; and

cryptographically encoding the divided segments using the cryptographic information corresponding to the transaction participants.

36. The system of claim 35, wherein the instructions having the method step of obtaining identities of at least two transaction participants comprise acquiring the identities from one of the transaction participants.

37. The system of claim 35, wherein the instruction having the method step of obtaining cryptographic information comprise acquiring cryptographic information from at least one of a directory and cryptographic identity provider.

38. The system of claim 35, wherein the instructions having the method step of dividing the information into segments comprise placing only a portion of the information which is needed by a particular transaction participant into a segment encrypted for the particular participant.

39. The system of claim 35, wherein the instructions performing the method further comprise:

transmitting a cryptographically encoded segment to only a cryptographically corresponding transaction participant.

40. The system of claim 35, wherein the instructions performing the method further comprise:

transmitting the cryptographically encoded segments to the at least two transaction participants.

41. A system comprising:

a processor having access to memory, the memory having instructions which, when executed, perform the method of controlling data content exposure in a multiparty transaction, the method comprising:

obtaining, from a primary transaction participant, at least two identities of secondary transaction participants to be involved in a multiparty transaction;

obtaining cryptographic information for the at least two secondary transaction participants, each secondary transaction participant having unique cryptographic information;

cryptographically encoding information for the at least two secondary transaction participants such that a data content and unique encryption are used for each secondary transaction participant; and

transmitting the cryptographically encoded information.

42. The system of claim 41, wherein the instructions performing the method step of transmitting the cryptographically encoded information comprise transmitting the cryptographically encoded information to the primary transaction participant.

43. The system of claim 41, wherein the instructions performing the method further comprise:

receiving status from the primary transaction participant concerning a successful examination of data content by one or more of the at least two secondary transaction participants, whereby multiparty transaction status is assessed.

44. The system of claim 41, wherein the instructions performing the method step of cryptographically encoding information for the at least two secondary transaction participants comprise encoding a data content that is unique for at least one of the at least two secondary transaction participants.

45. The method of claim 41, wherein the instructions performing the method steps further comprise transmitting a message request to act upon the information represented by the data content so as to execute the multiparty transaction.